МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МИРЭА – Российский технологический университет»

РТУ МИРЭА

Институт кибербезопасности и цифровых технологий

Кафедра КБ-1 «Защита информации»

Дисциплина: «Разработка защищённых автоматизированных систем»

Отчёт по практической работе № 2

Тема: «Разработка частного технического задания на создание автоматизированной информационной системы»

Вариант задания № 14

Выполнил

Студент группы БББО-05-20

Кутьин З.С.

14.04.2023

Проверил:

Головченко Д.А.

Москва 2023 г.

Вариант № 14: «Разработка защищенной автоматизированной информационной системы авиационно-спасательной компании МЧС России».

Учебная цель занятия: Углубить теоретические знания и выработать практические умения в области разработки технического задания на создание автоматизированных информационных систем с применением ГОСТ 19.201-78 «ЕСПД. Техническое задание. Требования к содержанию и оформлению» и ГОСТ 34.602-20 «Техническое задание на создание автоматизированной системы».

Место проведения занятия: компьютерная аудитория.

Учебно-материальное обеспечение:

1) Методическая разработка.
2) Компьютерный класс с ПЭВМ.
3) Операционная система семейства Windows.
4) Стандартный пакет MS Office или OpenOffice.org.

УТВЕРЖДАЮ

уководитель ФБГУ «АСК МЧС России»

_____ Д.А. Головченко

«__» _____ 202_ г.

ЧАСТНОЕ ТЕХНИЧЕСКОЕ ЗАДАНИЕ НА СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

автоматизированной информационной системы авиационно-спасательной компании МЧС России

СОГЛАСОВАНО

Руководитель группы разработки

_____ З.С. Кутьин

«__» _____ 202_ г.

Частное техническое задание на создание системы защиты автоматизированной информационной системы авиационно-спасательной компании МЧС России

1. Общие сведения

1.1. Полное наименование системы и ее условное обозначение

Полное наименование системы: система защиты автоматизированной информационной системы авиационно-спасательной компании МЧС России.

Краткое наименование системы: СЗИ АИС АСК.

1.2. Номер договора

Номер контракта: №1/32-54-76 от 24.03.2023

1.3. Наименование организаций Заказчика и Разработчика

Заказчиком системы является авиационно-спасательная компания МЧС России (далее – АСК)

Адрес заказчика: 121357, г. Москва, ул. Ватутина, 1.

Разработчиком системы является ЗАО «Разработчик».

Адрес разработчика: 563412, г. Москва, ул. Лесная, 18.

Заказчик: АСК.

1.4. Перечень документов, на основании которых создается система

- Приказ МЧС России от 22.02.2019 №100 «Об утверждении Положения об Управлении авиации и авиационно-спасательных технологий Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий»;
- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 1 ноября 2012 г. №1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21);

– ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;

1.5. Плановые сроки начала и окончания работы по созданию системы

Плановый срок начала работ по созданию защищенной автоматизированной информационной системы – 1 мая 2023 года;

Плановый срок окончания работ по созданию защищенной автоматизированной информационной системы – 1 января 2024 года.

1.6. Источники и порядок финансирования работ

Порядок финансирования определяется условиями контракта, источником финансирования является АСК МЧС России.

1.7. Порядок оформления и предъявления заказчику результатов работ по созданию системы

Система передается в виде функционирующего комплекса программных и аппаратных средств защиты информации, полностью интегрированных в действующую информационную систему.

Прием системы осуществляется комиссией в составе представителей заказчика, а также исполнителя.

Совместно с предъявлением системы производится сдача разработанного исполнителем комплекта документации.

2. Назначение и цели создания системы

2.1. Назначение системы защиты

Система защиты информации (СЗИ) АИС АСК предназначена для обеспечения безопасности ресурсов АИС в соответствии с требованиями федерального законодательства в сфере защиты информации, а также требованиями и рекомендациями полномочных органов исполнительной

власти Российской Федерации.

СЗИ АИС АСК должна обеспечивать следующие свойства защищаемой информации, обрабатываемой в АИС АСК:

- конфиденциальность информации (ресурсов автоматизированной информационной системы) – состояние информации (ресурсов автоматизированной информационной системы), при котором доступ к ней (к ним) осуществляют только субъекты, имеющие на него право;
- целостность информации (ресурсов автоматизированной информационной системы) – состояние информации (ресурсов автоматизированной информационной системы), при котором ее (их) изменение осуществляется только преднамеренно субъектами, имеющими на него право;
- доступность информации (ресурсов автоматизированной информационной системы) – состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовать их беспрепятственно.

СЗИ должна обеспечивать защиту информации от НСД, организацию ролевого доступа к информации, протоколирование, мониторинг состояния средств обеспечения информационной безопасности и отправку соответствующих уведомлений.

2.2. Цели создания системы защиты

Целью создания СЗИ АИС АСК является снижение вероятного ущерба от реализации угроз информационной безопасности и обеспечение устойчивого функционирования АИС АСК в соответствии с требованиями руководящих документов регулирующих органов, отечественных и международных стандартов по защите информации в автоматизированных системах обработки, хранения и передачи информации.

3. Характеристики объекта автоматизации

3.1. Краткие сведения об объектах автоматизации

Обработка защищаемой информации в АИС АСК осуществляется на

объекте Заказчика, расположенном по адресу: 121357, г. Москва, ул. Ватутина, 1.

Оператором АИС является АСК.

АИС является информационной системой персональных данных (ИСПДн). Количество субъектов ПДн превышает 100 000 субъектов.

В Системе обрабатываются ПДн, субъектов, не являющихся сотрудниками АСК, а также субъектов, являющихся сотрудниками АСК.

3.2. Описание технологии обработки информации

С документами, содержащими сведения ограниченного распространения, работают работники организации, имеющие соответствующую форму допуска и доступ к ресурсам ИСПДн.

Технологический процесс обработки информации в ИСПДн включает в себя:

- изготовление конфиденциальных документов, внесение конфиденциальной информации и персональных данных в базы данных АСК, просмотр и редактирование необходимой информации, печать документов на бумажном носителе, обмен файлами на машинных носителях информации по каналам связи;
- обеспечение необходимого уровня безопасности обработки, хранения и передачи конфиденциальной информации.

В подсистемах АИС реализована возможность настройки учётных записей пользователей АИС и их прав доступа (данный функционал доступен администраторам АИС). Вход пользователей в подсистемы АИС осуществляется по учетным данным (логину и паролю), отвечающим требованиям парольной политики, разработанной Оператором АИС.

На объект информатизации АРМ пользователя установлена операционная система Windows 10. Информационная система, в которой обрабатывается защищаемая информация, размещена в изолированной подсети от остальной локальной сети АСК, средствами межсетевого экрана, в отдельном VLAN.

Режим обработки информации в АИС – многопользовательский с разграничением прав доступа.

3.3. Объекты защиты в АИС

В АИС объектами защиты являются:

- информация, обрабатываемая в АИС;
- технологическая и служебная информация, связанная с функционированием АИС;
- технические средства обработки информации, системное и прикладное программное обеспечение АИС;
- программно-аппаратные комплексы и программные средства защиты информации и криптографические средства защиты информации, входящие в состав АИС;
- машинные носители информации;
- каналы связи, выходящие за пределы контролируемой зоны.

4. Требования к системе

4.1. Требования к системе в целом

Совокупность программно-технических средств СЗИ и поддерживающие их организационные меры должны обеспечивать защиту конфиденциальной информации, обрабатываемой в АИС, от угроз безопасности информации, а также должна обеспечивать выполнение требований нормативных документов ФСТЭК России и ФСБ России, в части безопасности информации.

Согласно постановлению правительства № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» АИС, обрабатывающая персональные данные как сотрудников АСК, так и пострадавших, имеет уровень защищенности персональных данных 1 уровня, так как количество обрабатываемых субъектов более 100 000, а тип актуальных угроз 1.

В СЗИ АИС АСК должны быть реализованы меры защиты информации, предъявляемые к государственным информационным системам 2 класса

защищенности, а в соответствии с положениями приказа ФСТЭК России от 18.02.2013 г. № 21, включающие в себя:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;
- обнаружение вторжений;
- контроль (анализ) защищенности информации;
- обеспечение целостности информационной системы и информации;
- обеспечение доступности информации;
- защиту технических средств;
- защиту информационной системы, ее средств, систем связи и передачи данных.

в соответствии с:

– угрозами безопасности информации;

– требованиями Приказа ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

В соответствии с п. 12 Приказа ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», для построения СЗИ АИС АСК необходимо использовать средства, которые должны быть сертифицированы на соответствие обязательным требованиям по безопасности информации, установленным нормативными правовыми актами, или требованиям, указанным в технических условиях (заданиях по

безопасности).

4.1.1. Требования по идентификации и аутентификации субъектов доступа и объектов доступ

Применяемые для построения СЗИ АИС АСК организационные и технические меры должны обеспечивать:

– идентификацию, аутентификацию и авторизацию пользователей в операционной системе автоматизированного рабочего места (АРМ) сотрудника, а также идентификацию, аутентификацию и авторизацию пользователей в системе управления базами (СУБД) АИС АСК. Процесс «Выполнить аутентификацию» состоит непосредственно из ввода логина и пароля, после чего системой проверяется правильность ввода данных. После проверки введенных данных, если предоставленные данные были неверны, система проверяет число допустимых ошибок и, если число допустимых ошибок меньше заданного значения, система позволяет еще раз ввести логин и пароль, иначе будет выведено сообщение о несанкционированном доступе с последующий блокировкой.

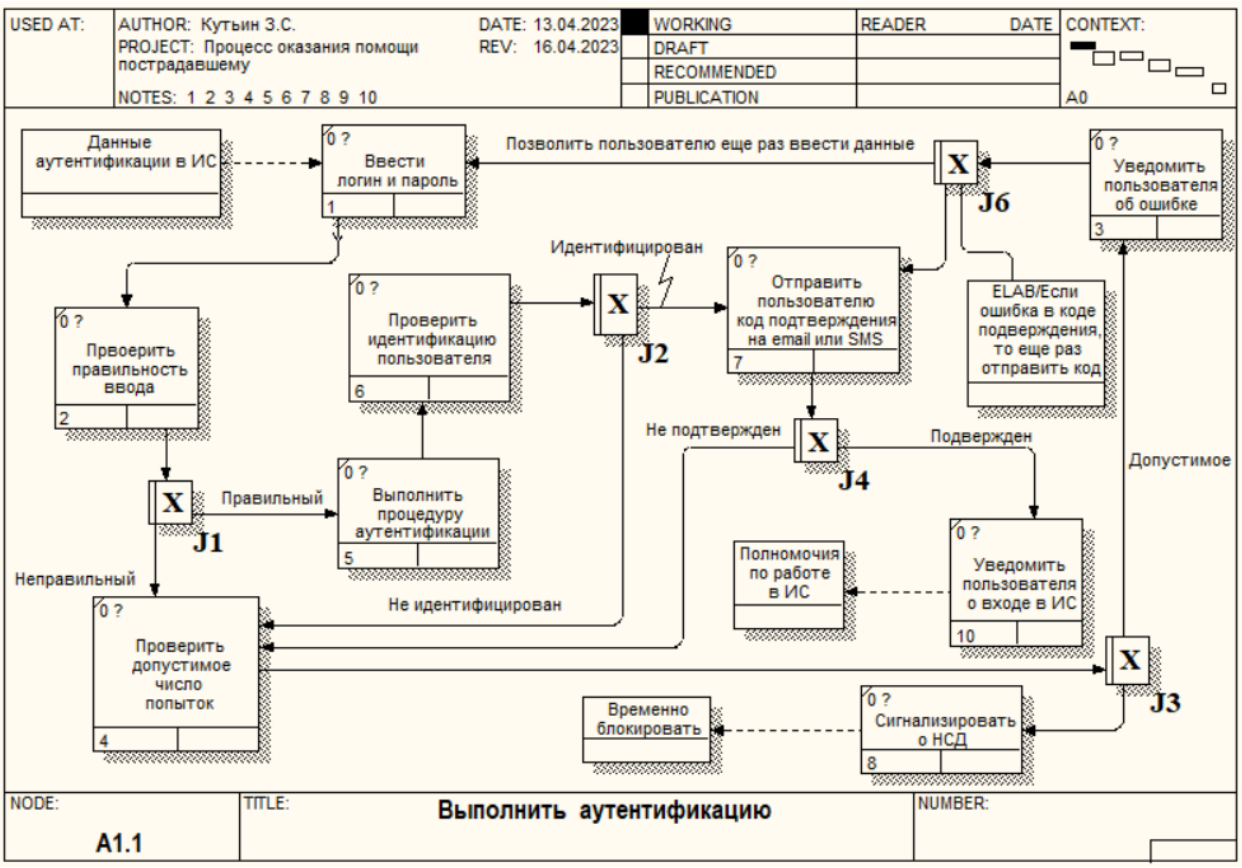

Рисунок 1 - Диаграмма декомпозиции работы «Выполнить аутентификацию

– идентификацию, аутентификацию и авторизацию пользователей в операционной системе автоматизированного;

– управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;

– управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации.

4.1.2. Требования по управлению доступом субъектов доступа к объектам доступа

Применяемые для построения СЗИ АИС АСК организационные и технические меры должны обеспечивать:

– Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей;

– Реализацию дискреционного и ролевого правила разграничения

доступа на чтение, запись, выполнение;

– Управление (фильтрация, маршрутизация, контроль соединений) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами;

– Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;

– Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;

– Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе);

– Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя;

– Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации;

– Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети;

– Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы).

Для управления информационными потоками в СЗИ АИС АСК должны применяться межсетевые экраны (МЭ) не ниже 6 класса защиты, согласно требованиям, информационного сообщения ФСТЭК России от 28 апреля 2016 г. №240/24/1986 «Об утверждении требований к межсетевым экранам».

4.1.3. Требования по защите машинных носителей информации

Применяемые для построения СЗИ АИС АСК организационные и технические меры должны обеспечивать:

– Уничтожение (стирание) или обезличивание информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения

(стирания) или обезличивания.

4.1.4. Требования по регистрации событий безопасности

Применяемые для построения СЗИ АИС АСК организационные и технические меры должны обеспечивать:

– Определение событий безопасности, подлежащих регистрации, и сроков их хранения;

– Определение состава и содержания информации о событиях безопасности, подлежащих регистрации;

– Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;

– Защита информации о событиях безопасности.

4.1.5. Требования по антивирусной защите

Применяемые для построения СЗИ АИС АСК организационные и технические меры должны обеспечивать:

– Реализацию антивирусной защиты;

– Обновление базы данных признаков вредоносных компьютерных программ (вирусов).

Для обеспечения антивирусной защиты СЗИ АИС АСК должны применяться средства антивирусной защиты (САВЗ) не ниже 4 класса и 4 уровня доверия, согласно требованиям, п. 12 Приказа ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

4.1.6. Требования по обеспечению целостности

Применяемые для построения СЗИ АИС АСК организационные и технические меры должны обеспечивать:

– Возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций.

4.1.7. Требования по защите технических средств

Применяемые для построения СЗИ АИС АСК организационные и технические меры должны обеспечивать:

– Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены;

– Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.

4.1.8. Требования по защите передачи данных

Применяемые для построения СЗИ АИС АСК организационные и технические меры должны обеспечивать:

– Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны.

Для обеспечения защиты передачи данных СЗИ АИС АСК по каналам связи, имеющим выход за пределы контролируемой зоны должны применяться средства криптографической защиты информации (СКЗИ) не ниже класса КС1 с учетом результатов разработки «Модели угроз и нарушителя безопасности информации».

4.2. Требования к структуре и функционированию

Совокупность программно-технических средств СЗИ АИС АСК и поддерживающие их организационные меры должны обеспечивать защиту информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, обрабатываемой в АИС АСК, от угроз безопасности, приведенных в Модели угроз безопасности.

Состав подсистем СЗИ АИС АСК и выполняемые ими функции

представлены в таблице 1.

Таблица 1 – Состав подсистем СЗИ АИС АСК

№ п/п	Наименование подсистемы	Функции подсистемы
1.	Подсистема управления доступом	– идентификация и аутентификация пользователей, устройств; – управление идентификаторами, средствами аутентификации; – управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей; – реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа; – разделение полномочий (ролей) пользователей.
2.	Подсистема регистрации и учета	– регистрация и учет событий безопасности; – контроль установки обновлений программного обеспечения, работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации; – контроль состава технических средств, программного обеспечения и средств защиты информации; – контроль правил генерации и смены паролей пользователей; – учет машинных носителей информации.

Продолжение таблицы 1

№ п/п	Наименование подсистемы	Функции подсистемы
3.	Подсистема обеспечения целостности	– контроль целостности программного обеспечения, персональных данных; – обеспечение возможности восстановления программного обеспечения; – обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений; – контроль содержания информации, передаваемой из информационной системы; – ограничение прав пользователей по вводу информации в информационную систему; – выполнение резервного копирования защищаемой информации.
4.	Подсистема межсетевого экранирования	– защита процессов функционирования информационной системы при передаче данных по каналам связи; – обеспечения межсетевого экранирования.
5.	Подсистема обеспечения антивирусной защиты	– антивирусная защита; – обновление базы данных признаков вредоносных компьютерных программ (вирусов).
6.	Подсистема анализа защищенности	– анализ потенциального воздействия планируемых изменений в конфигурации; – управление изменениями конфигурации информационной системы и системы защиты персональных данных.
7.	Подсистема защиты виртуализации	– идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре; – управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре; – регистрация событий безопасности в виртуальной инфраструктуре; – реализация и управление антивирусной защитой в виртуальной инфраструктуре.

4.3. Требования к численности и квалификации персонала системы и режиму его работы

Обслуживающий персонал должен состоять из администраторов СЗИ ЗАИС АСК – лиц, ответственных за функционирование СЗИ АИС АСК в установленном штатном режиме.

Проектные решения по созданию СЗИ АИС АСК должны содержать

(при необходимости) рекомендации к изменению численности, квалификации и функциям персонала, предложения по обучению обслуживающего персонала СЗИ АИС АСК с учетом существующей организационно-штатной структуры АСК и разграничения ролей по реализации политики безопасности и обслуживанию технических средств СЗИ АИС АСК.

Обслуживающий персонал СЗИ АИС АСК должен осуществлять обслуживание и эксплуатацию СЗИ АИС АСК по рабочим дням в рабочее время с возможностью выхода в нерабочее время для проведения сервисного обслуживания или восстановления работоспособности СЗИ АИС АСК.

4.4. Показатели назначения

Техническими и организационно-распорядительными мерами должна быть обеспечена безопасность информации при ее обработке в СЗИ АИС АСК, а именно обеспечены конфиденциальность, целостность и доступность защищаемой информации.

СЗИ создаваемой СЗИ АИС АСК должны обеспечивать возможное расширение круга защищаемых ресурсов, добавление или удаление объектов защиты.

4.5. Требования к надежности

Надежность СЗИ АИС АСК должна быть обеспечена за счет ведения двух копий программных СЗИ, создания резервных копий настроек СЗИ, их периодического обновления и контроля работоспособности.

4.6. Требования безопасности

При вводе в действие оборудования СЗИ АИС АСК с учетом требований стандартов безопасности труда должна быть обеспечена безопасность при монтаже, наладке, эксплуатации, обслуживании и ремонте оборудования СЗИ АИС АСК, включая защиту от воздействий электрического тока, электромагнитных полей, акустических шумов.

Размещение оборудования СЗИ АИС АСК на штатных местах должно обеспечивать его безопасное обслуживание и эксплуатацию.

4.7. Требования к эргономике и технической эстетике

Программно-аппаратные компоненты, внедряемые при создании СЗИ АИС АСК, не должны существенно нарушать удобство работы эксплуатирующего персонала.

4.8. Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов системы

Климатические условия эксплуатации компонентов СЗИ АИС АСК должны соответствовать требованиям эксплуатационной документации производителей СЗИ.

Эксплуатация программно-технических средств должна предусматривать следующие виды технического обслуживания:

– оперативное обслуживание;

– профилактические работы.

Оперативное обслуживание должно предусматривать ежедневный контроль функционирования аппаратно-технических средств, целостности информационных ресурсов. Оперативное обслуживание не должно нарушать выполнения функций СЗИ АИС АСК в целом.

Профилактические работы должны включать в себя периодическую проверку и обслуживание технических средств СЗИ ЗАИС АСК, для которых такое обслуживание и процедуры предусмотрены эксплуатационной документацией.

Объем и порядок выполнения технического обслуживания технических и программных средств СЗИ АИС АСК должны определяться эксплуатационной документацией производителя на СЗИ.

4.9. Требования по сохранности информации при авариях

Сохранность информации при авариях должна быть обеспечена СЗИ АИС АСК за счет резервного копирования обрабатываемой информации.

При авариях в СЗИ АИС АСК должна быть обеспечена сохранность следующей информации:

– о собранных событиях информационной безопасности;

– о настройках компонентов СЗИ АИС АСК.

Для обеспечения сохранности информации при авариях разрабатываемый технический проект на создание СЗИ АИС АСК должен предусматривать средства восстановления, а также мероприятия по ведению копий программных СЗИ, их периодическому обновлению и контролю работоспособности.

4.10. Требования к защите от влияния внешних воздействий

Требования по стойкости, устойчивости и прочности к внешним воздействиям (среде применения) для компонентов СЗИ АИС АСК не предъявляются.

4.11. Требования к патентной чистоте

Технические решения по созданию СЗИ АИС АСК должны отвечать требованиям действующего российского законодательства об авторском праве и смежных правах по патентной чистоте.

4.12. Требования по стандартизации и унификации

Должна обеспечиваться совместимость технических средств и программного обеспечения СЗИ ЗАИС АСК с комплексом технических средств АИС АСК.

При создании СЗИ АИС АСК должны использоваться унифицированные, однотипные компоненты в целях снижения расходов на обслуживание и ремонт, обеспечения удобства эксплуатации.

4.13. Требования к функциям

Состав функций подсистем СЗИ АИС АСК приведен в разделе 4.2. Для реализации функций СЗИ АИС АСК должны использоваться:

- встроенные средства защиты информации – возможности и механизмы защиты информации, предоставляемые операционной системой (ОС), СУБД, прикладным ПО, телекоммуникационным и сетевым оборудованием, сертифицированные по требованиям безопасности информации Российской Федерации;
- дополнительные (специализированные) СЗИ, предназначенные для выполнения требований по безопасности информации, не реализуемые

встроенными СЗИ. Выбор дополнительных СЗИ должен производиться в проекте СЗИ АИС АСК, на основе анализа возможностей по защите информации встроенных СЗИ и требований к подсистемам СЗИ АИС АСК;

- организационные мероприятия по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну.

Для определения конкретных требований к функциям СЗИ АИС АСК из множества угроз (определенных в модели угроз) выделяются компоненты (уязвимости, способы реализации угроз, деструктивные действия, источники, каналы утечки), на нейтрализацию которых будут направлены требования.

Организационные и технические меры, направленные на защиту информации, должны быть реализованы посредством реализации следующих функциональных подсистем:

– подсистема защиты от несанкционированного доступа (далее — НСД);

– подсистема антивирусной защиты;

– подсистема криптографической защиты информации;

– подсистема межсетевого экранирования.

Все компоненты подсистем должны интегрироваться в существующую ИТ-инфраструктуру АСК.

4.13.1. 2.Требования к подсистеме защиты от НСД

К подсистеме защиты от НСД предъявляются следующие требования:

– обеспечение защиты от несанкционированного входа в систему на защищаемых АРМ;

– обеспечение разграничения доступа пользователей к информационным ресурсам на основе избирательного разграничения доступа и замкнутой программной среды;

– обеспечение контроля и предотвращения несанкционированного изменения целостности защищаемых ресурсов;

– регистрация событий информационной безопасности в

собственном журнале;

– обеспечение возможности просмотра сведений, произошедших на защищаемых АРМ;

– обеспечение возможности контроля вывода на печать конфиденциальной информации;

– обеспечение возможности доверенного удаления файлов без возможности последующего восстановления;

– обеспечение возможности управления доступом пользователей к защищаемым АРМ.

4.13.2. Требования к подсистеме антивирусной защиты

К подсистеме антивирусной защиты предъявляются следующие требования:

– обеспечение защиты от воздействия вредоносного кода на защищаемые ресурсы;

– обеспечение возможности удалённой централизованной установки и удаления компонент подсистемы на защищаемых ресурсах;

– обеспечение возможности централизованного управления компонентами подсистемы;

– обеспечение возможности автоматического централизованного обновления антивирусных баз на защищаемых ресурсах;

– обеспечение возможности централизованного сбора статистических отчётов о работе компонент подсистемы, событий информационной безопасности;

– обеспечение возможности оповещения администратора информационной безопасности о критичных событиях.

4.13.3. Требования к подсистеме криптографической защиты информации

К подсистеме криптографической защиты информации предъявляются следующие требования:

– обеспечение возможности шифрования/расшифрования

информации, передаваемой за пределы контролируемой зоны, с использованием алгоритма шифрования ГОСТ 28147-89 с применением сертифицированных ФСБ России средств криптографической защиты информации;

– реализация технологий и поддержка постоянно действующих туннелей виртуальной частной вычислительной сети (VPN);

– обеспечение возможности проверки подлинности отправителя (удаленного пользователя) и целостности, передаваемых по информационно-телекоммуникационной сети международного информационного обмена (сети связи общего пользования) данных с использованием криптоалгоритмов;

– организация контролируемого и безопасного подключения внешних пользователей для защищенного обмена информацией, в том числе аутентификацию пользователей и сетевых объектов с использованием криптоалгоритмов.

4.13.4. Требования к подсистеме межсетевого экранирования

К подсистеме межсетевого экранирования предъявляются следующие общие требования:

- сетевое сегментирование СЗИ АИС АСК в целях локализации защищаемых информационных ресурсов по степени критичности и реализация механизмов контроля доступа между сегментами на сетевом уровне;
- разделение информационных взаимодействий между сегментами СЗИ ЗАИС АСК и внешними сетями общего пользования.

Для выполнения общих требований подсистема межсетевого экранирования должна обеспечивать:

– фильтрацию пакетов на сетевом уровне на основе сетевых адресов отправителя и получателя;

– фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

– фильтрацию пакетов с учетом входного и выходного сетевого интерфейса, как средство проверки подлинности сетевых адресов;

– регистрацию и учет фильтруемых пакетов;

– регистрацию сведений об установленных сессиях;

– трансляцию сетевых адресов;

– разграничение сетевых потоков с использованием виртуальных контекстов в рамках одного устройства или отдельных устройств;

– маршрутизацию пакетов между сегментами СЗИ АИС АСК;

– маршрутизацию пакетов или NAT в сетевые сегменты СЗИ АИС АСК из локальной сети АСК, открытого сегмента сети АСК и сетей общего пользования.

4.13.5. Требования к подсистеме анализа защищенности

К подсистеме анализа защищенности предъявляются следующие требования:

– обеспечение возможности сбора информации о доступности узлов СЗИ ЗАИС АСК;

– обеспечение возможности обнаружения сетевых узлов, идентификации операционных систем;

– обеспечение возможности выявления уязвимостей в сетевых службах и приложениях в режиме тестирования на проникновение;

– обеспечение возможности оценки защищенности баз данных;

– обеспечение возможности проверки безопасности операционной системы и приложений на защищаемых ресурсах;

– обеспечение возможности установления различных правил политик безопасности для различных сетевых узлов;

– обеспечение контроля учетных записей и групп пользователей баз данных и приложений, объектов баз данных.

4.14. Требования к видам обеспечения

4.14.1. Требования к программному обеспечению

Дистрибутивное программное обеспечение СЗИ АИС АСК должно

храниться на внешних носителях с инструкцией и программой инсталляции.

Программные средства защиты и их компоненты, устанавливаемые на рабочие станции СЗИ АИС АСК, должны функционировать в среде используемых на них операционных систем.

При выборе программных средств защиты предпочтение должно отдаваться готовым покупным программным продуктам.

В процессе эксплуатации СЗИ АИС АСК лицензии на дополнительные функции программного обеспечения должны поддерживаться в актуальном состоянии, т.е. необходимо регулярное их обновление.

Решения по использованию программных средств защиты должны приниматься с учетом обеспечения поддержки его функционирования производителем или поставщиком данного программного обеспечения.

Предлагаемое к использованию программное обеспечение должно быть лицензировано фирмой-производителем или являться авторизованной копией, изготовленной установленным порядком.

4.14.2. Требования к техническому обеспечению

Аппаратные компоненты СЗИ АИС АСК и автоматизированные рабочие места администраторов должны базироваться на аппаратных платформах, обеспечивающих функции диагностики, резервирования и взаимозаменяемости.

При выборе и закупке аппаратных компонентов СЗИ АИС АСК должны быть предусмотрены мероприятия по их последующему гарантийному и техническому обслуживанию.

5. Состав и содержание работ по созданию системы защиты

В рамках настоящего технического задания в составе работ по созданию СЗИ АИС АСК предусматриваются следующие стадии:

Стадия 1. Формирование требований к защите информации, обрабатываемой в АИС АСК;

Стадия 2. Разработка документации;

Стадия 3. Выбор оборудования и программного обеспечения,

его инсталляция в состав СЗИ АИС АСК;

Стадия 4. Внедрение СЗИ АИС АСК.

6. Требования к составу и содержанию работ по подготовке объекта автоматизации к вводу системы в действие

6.1. Требования к стадии формирования требований к защите информации, обрабатываемой в АИС АСК

Формирование требований к защите информации, обрабатываемой в рамках АИС АСК, осуществляется с учетом ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» (далее - ГОСТ Р 51583) и ГОСТ Р 51624 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования» (далее - ГОСТ Р 51624) и в том числе включает:

- определение класса АИС АСК;
- определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в АИС АСК, и разработку на их основе модели угроз безопасности информации;
- определение детальных требований к Системе ЗИ.

6.2. Требования к стадии разработки документации

Разработка СЗИ АИС АСК должна осуществляться в соответствии с частным техническим заданием на создание СЗИ АИС АСК с учетом ГОСТ 34.601 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания» (далее - ГОСТ 34.601), ГОСТ Р 51583 и ГОСТ Р 51624.

Разработка СЗИ АИС АСК должна включать следующие стадии:

- проектирование СЗИ АИС АСК;
- разработка организационно-эксплуатационной документации на Систему ЗИ;
- разработка комплекта эксплуатационной документации на Систему ЗИ.

Система ЗИ не должна препятствовать достижению целей создания АИС АСК и ее функционированию.

При разработке СЗИ АИС АСК должно учитываться ее информационное взаимодействие с иными информационными системами и информационно-телекоммуникационными сетями.

6.3. Требования к программным и аппаратным средствам ЗИ

Требования к техническому обеспечению

Программные и аппаратные СрЗИ СЗИ АИС АСК должны снабжаться обязательствами технической поддержки (сертификатами, контрактами и т.п.) сроком не менее одного года.

Требования к программному обеспечению

Специальное программное обеспечение СЗИ АИС АСК и его компоненты, устанавливаемые на АИС АСК, должны функционировать в среде используемых на них ОС. Специальное программное обеспечение СЗИ АИС АСК должно обеспечивать возможность адаптации к изменению конфигурации ПТС, в том числе к введению нового оборудования АИС АСК. Все программное обеспечение СЗИ АИС АСК должно использоваться с комплектами соответствующих лицензий и контрактами (сертификатами) технической поддержки сроком не менее 1 года.

Требования к методическому и организационному обеспечению

Методическое и организационное обеспечение СЗИ АИС АСК должно соответствовать требованиям руководящих и нормативных документов ФСТЭК России и ФСБ России и включать комплект необходимой организационно-распорядительной документации (ОРД) в части защиты информации, не содержащей сведений, составляющих государственную тайну.

6.4. Требования к стадии внедрения

При подготовке к вводу в действие СЗИ АИС АСК Разработчик должен подготовить и согласовать с Заказчиком список технических средств, доступ к которым должен быть предоставлен для ввода в действие СЗИ АИС АСК.

При подготовке к вводу в действие СЗИ АИС АСК Заказчик должен обеспечить:

- предоставление доступа к компонентам АИС АСК сотрудникам Разработчика;
- готовность инфраструктуры к установке компонентов СЗИ АИС АСК;
- наличие обученного персонала для обеспечения эксплуатации компонентов СЗИ АИС АСК;
- утверждение ОРД, созданной на стадии разработки ОРД по защите ограниченного доступа, не содержащей сведения, составляющие государственную тайну;
- издание приказов о формировании соответствующих приемочных комиссий по вводу в действие СЗИ АИС АСК.

7. Порядок контроля и приемки СЗИ

Сдача-приёмка работ должна производиться поэтапно, в соответствии с календарным планом, являющимся дополнением к договору между заказчиком и исполнителем.

По окончанию каждого этапа исполнитель должен предоставить заказчику указанные результаты работ. При завершении каждого этапа исполнитель и заказчик должны подписывать акт сдачи-приемки.

Конечный срок сдачи работ 1 января 2024.

8. Требования к документированию

Разработка документации должна вестись в соответствии с ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначения документов при создании автоматизированных систем».

Передача разработанной документации для согласования, через открытые каналы связи без шифрования – запрещена.

Результаты оказания работ передаются комплектом документов, который должен быть передан на бумажном носителе и в электронном виде

(форматы *.docx, *.pdf, *.vsd) Заказчику.